

EXHIBIT A

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

**U.S. SECURITIES AND EXCHANGE
COMMISSION,**

Plaintiff,

v.

**VLADISLAV KLIUSHIN (a/k/a
VLADISLAV KLYUSHIN), *et al.*,**

Defendants.

Case No. 1:21-cv-12088-WGY

DECLARATION OF CONNOR R. HURLEY

I, Connor R. Hurley, pursuant to 28 U.S.C. § 1746, declare as follows:

I. Qualifications

1. I am a Financial Economist in the Division of Economic and Risk Analysis (“DERA”) of the U.S. Securities and Exchange Commission (“SEC” or “Commission”). I joined the Commission in 2014 as a Presidential Management Fellow. In the last nine years, I have assisted the Commission in numerous enforcement investigations. My work consists of performing financial, economic, statistical, and quantitative analyses in the context of those investigations. As part of my work, I frequently analyze trading records and conduct financial analyses and statistical analyses of trading patterns. I have served as an expert witness and supported experts in both civil and criminal actions conducting similar analyses.

2. I have a Master of Public Policy degree from the University of Chicago and a Bachelor of Arts degree, with a major in Economics, from the State University of New York at Geneseo. I have completed undergraduate and graduate coursework in econometrics, statistics, applied regression analysis, and data science as part of both my undergraduate and graduate education.

II. Scope

3. I was asked by Commission staff to assess trading activity over the period January 1, 2018 through September 30, 2020 (the “Relevant Period”) conducted in 22 brokerage accounts affiliated with the Defendants, other individuals in whose accounts the Defendants traded, and M13 (the IT Company identified in the Complaint), all of which were identified as having trades associated with the hack-to-trade scheme alleged in this case (collectively, the “Accounts”). More specifically, I was asked to perform quantitative and statistical analyses of the trading activity in the Accounts to determine (1) the profit generated on trades associated with the scheme and (2) if the trading patterns and outcomes exhibit a statistical relationship to financial filings prepared by two service-provider firms for various companies that were hacked as part of the scheme. This Declaration is based on my experience, training, and analyses of the filings and trading activity in the Accounts.

III. Data Sources

4. My analyses are based on the following data sources:

- a. Records provided by broker dealers of securities transactions in the Accounts.

The records contain details on the security type (stock, option, contract for difference (“CFD”), and others), buy/sell side, price, and quantity, among other information. These Accounts are associated with the Defendants, other individuals in whose accounts the Defendants traded, and M13 (the IT Company identified in the Complaint), as set out in Table 1, and were used to conduct the trading associated with the scheme.

- b. Financial data, including daily securities price information from the Center for Research in Security Prices (“CRSP”), a publicly available commercial database.
- c. Quarterly company earnings information and analyst earnings expectations from Institutional Brokers’ Estimate System (“IBES”), a publicly available commercial database.
- d. EDGAR filings for the Relevant Period. This data contains information filed with the SEC through the Commission’s Electronic Data Gathering, Analysis and Retrieval (“EDGAR”) system, including the type of financial filing, the reporting company, the company that submitted the filing, and the date the filing was accepted. This data is publicly available from the SEC’s EDGAR archives. This data was supplemented with information from a publicly available database produced by Compustat, which includes additional information about the time the filing was published.

IV. Trades, Earnings, and Potentially Hack Related Trading

5. Roundtrip Database: I constructed a database of ‘roundtrip’ transactions in each Account from the Account’s transaction data. The roundtrip database serves as the basis for my trading analysis. A ‘roundtrip’ is a transaction that is opened when a new position, either long or short is initiated, combined with the subsequent closing of the position. Each roundtrip in the database is characterized by Account; the ticker of the security (or underlying security in the case of CFD transactions); whether the position was long or short; the open and closing time, the length of time the position was open; and the profits (or losses) earned.

6. Earnings Indicator: Each roundtrip transaction was flagged as being related to a reporting company's public quarterly earnings announcement if two conditions were both satisfied. First, the roundtrip had to be opened before the reported earnings announcement time, but no more than three trading days earlier. For example, for a public earnings announcement made at 4:00 PM on a Wednesday, the opening of the position would have to be no earlier than the preceding Monday. Second, the position had to be closed after the public earnings announcement time. In other words, the roundtrip had to straddle the public earnings announcement.

7. Potential Hack Related Trade Indicator: Each roundtrip transaction in a security was flagged as being potentially related to the hack of the two service-provider firms alleged to be hacked in the scheme in this case if the following conditions were met. First, there had to be a financial filing (a Form 8-K, 10-K, 10-Q, 6-K, 20-F, 40-F, or amended version thereof), which was filed by one of the two hacked service-provider firms for one of its company clients. Forms were identified as being filed by a service-provider firm when one of the unique codes associated with the service-provider form was present in the financial filing's accession number.¹ The filing had to occur within plus or minus three trading days from a reporting company's quarterly earnings announcement as recorded in the IBES database. Second, the financial filing had to occur after a roundtrip position had been opened. If the filing around which the trading occurred was not filed by a hacked service-provider firm, or if a service-

¹ An accession number is a unique identifier assigned automatically to an accepted submission by the EDGAR Filer System. The first 10 digits comprise the Central Index Key (CIK) of the entity submitting the filing. This could be the company or a third-party filer agent, depending on who submitted the filing. The CIK numbers for the service-provider firms used to identify relevant filings are: 0001558370, 0001104659, 0001144204, 0001047469, 0001410578, 0001571049, 0001564590, 0001193125, 0000950123, and 0001299933.

provider filing only occurred prior to the opening of a position, the roundtrip transaction would not be flagged as a Potentially Hack Related Trade.

8. The analysis showed that there may have been several roundtrip transactions associated with one earnings event. I combined these roundtrip trades in a given security that opened up to three business days prior to an earnings event and remained open until after the earnings event into one trading episode. For example, a position opened on Monday at 10:00 AM in one account and another position opened on Tuesday at 11:00 AM, with both being closed after the earnings announcement on Wednesday at 4:00 PM, would combine into one episode. This aggregation of trading into episodes was used to analyze the transactions around each earnings announcement. Similarly, I aggregated roundtrip transactions around earnings events that are not Potentially Hack Related (“Other Trades”) into trading episodes.

V. Profits from Potentially Hacked Trading Episodes

9. Table 2 shows the performance and overall profitability for trading episodes that were Potentially Hack Related Trades, as described in paragraph 7 above, for each Account.

10. The Amount Open is the total amount traded in all Potentially Hacked Trading Episodes. The Win Rate is the percent of trading episodes that were profitable.

11. Gross MacDonald Profits: The final column of Table 2 shows the gross *MacDonald* Profits, which is the basis for the requested disgorgement amounts. *See SEC v. MacDonald*, 699 F.2d 47, 54 (1st Cir. 1983). The gross *MacDonald* Profits are calculated using the next closing price for the stock following an earnings announcement, if the position has not already been closed, and do not include episodes that result in net losses. For example, if a roundtrip transaction opened prior to an earnings announcement made on Tuesday at 8:00 AM and closed prior to the market close on Tuesday at 4:00 PM (the next closing price after the earnings

announcement), the *MacDonald* Profits are based on the transaction price of the closing trade. However, if the roundtrip was not closed by 4:00 PM, the Tuesday market closing price would be used to calculate the *MacDonald* Profits. Similarly, if the roundtrip was opened prior to an earnings announcement on Tuesday at 6:00 PM and was not closed by Wednesday at 4:00 PM (the next closing price after the earnings announcement), the closing price for the security on Wednesday would be used to calculate the *MacDonald* Profits. Based on this analysis, I calculated the gross *MacDonald* Profits sum for all of the Account trades associated with the scheme to be \$121,923,901.

12. The current profits analysis is greater than the \$82.5 million alleged in the SEC Complaint because it applies the *MacDonald* methodology for calculating disgorgement in insider trading cases for the entire time period of January 2018 to September 2020 when evidence identified in this case and the parallel criminal proceedings shows trades associated with the scheme occurred. In addition, this analysis incorporates information from additional trade blotters received after the Complaint was filed that includes additional trading associated with the scheme.

13. Comparison of Potentially Hack Related Trades to Other Trades: During the Relevant Period, the Accounts invested 3.3 times more in Potentially Hack Related Trades, over \$2.21 billion, than in Other Trades, about \$0.66 billion. Overall, the Other Trades were not profitable, resulting in a net loss of over \$8.2 million.

14. Prejudgment Interest: Commission staff asked me to calculate prejudgment interest (“PJI”) on the disgorgement amounts for Defendants Sladkov, Irzak, and Rumiantcev through October 31, 2023. For each of these Defendants, I determined the gross *MacDonald* Profits described above for each quarter and calculated the appropriate PJI through October 31, 2023,

applying an assumption that each Potentially Hack Related Trade occurred on the last day of the quarter after the relevant earnings announcement. I applied the interest rate used by the Internal Revenue Service for underpayments, compounding interest quarterly.

15. The total PJI on the disgorgement amounts for Defendants Sladkov, Irzak, and Rumiantcev can be found in Table 3, followed by the detailed quarterly calculations.

VI. Propensity to Trade in Potentially Hack Related Events

16. I performed a statistical test to evaluate whether each Account was more likely to trade on earnings events that had financial filings prepared by one of the two hacked service-provider firms than earnings events that did not have financial filings prepared by the hacked service-provider firms. Table 4 shows the inputs for the test and the results of the test for each Account. The first four columns contain: (1) the number of all quarterly earnings events from the IBES database that were made during the segment of time during the Relevant Period when the Account was actively trading; (2) the number of those events (a subset of the total number) that was filed by one of the two hacked service-provider firms; (3) the number of earnings events that the Account traded around; and (4) the number of earnings events that the Account traded around that were filed by a service-provider firm. For example, a total of 46,869 earnings events occurred during the period of trading in Sladkov's Accounts. Of those events, 20,589 (or 44 percent) were filed by one of the two hacked service-provider firms. Sladkov's Accounts traded on 386 events, of which 375 (or 97 percent) were filed by one of the two hacked service-provider firms.

17. In the fifth column of Table 4, I calculated the number of Potentially Hack Related Events the Accounts would have been expected to trade around under the assumption that the Accounts trading activity was uncorrelated with (or independent of) the hacked service provider

firms. For example, given that Sladkov's Accounts traded 386 of the 46,869 total earnings events, the expectation would be that these Accounts would have traded 170 of the events associated with the service-provider filings. In fact, these Accounts traded in 375 events associated with the service provider filings, more than twice as many as would be expected. Although the two hacked service provider firms were only involved in 44 percent of the filings, the Accounts almost exclusively traded (more than 95 percent) around earnings announcements submitted by these hacked service provider firms.

18. The final column of Table 4 shows the result of a statistical test—the Fisher Exact Test—for whether the disproportionate Potentially Hack Related Trades exhibited by the Accounts could have arisen by random chance. The p-value from the test measures the probability that the trading pattern could have occurred by chance. The smaller the p-value, the less likely it is that the outcome could have occurred by chance. A p-value of 0.05 (chances of 5-in-100 that the outcome could have occurred by chance) is a commonly used threshold in academic studies and in litigation matters for concluding that an outcome did not occur by chance. For all of the Accounts, the Potentially Hacked Related Trades was so concentrated that the largest p-value among them is far less than one in one trillion. This means that it is nearly impossible that the Accounts trading is uncorrelated to the role of a hacked service-provider submitting the earnings announcements of the public companies whose securities the traders traded.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on December 14, 2023.

/s/ Connor Hurley
Connor R. Hurley

Table 1: Accounts Associated with Scheme

Igor Sladkov	285 [REDACTED]	2959 [REDACTED]	[REDACTED] 00	
Vladislav Klyushin	33145 [REDACTED]	[REDACTED] 8	[REDACTED] 19	[REDACTED] 586, 873, 919, 922, 923
Alexander Borodaev	34227 [REDACTED]	[REDACTED] 42		
Sergey Uryadov	34220 [REDACTED]	[REDACTED] 97		
Mikhail Irzak	23778 [REDACTED]	[REDACTED] ETR	[REDACTED] 120557	[REDACTED] 96
Boris Varshavskiy	[REDACTED] 40			
Rumiantcev	[REDACTED] 4			
M13	[REDACTED] 27			

Table 2: Trading Summary			
Accounts	Potentially Hacked Trading		
	Amount Open	Win Rate	Gross <i>MacDonald</i> Profits
Igor Sladkov	\$803,823,138	69.3%	\$50,864,250
Vladislav Kliushin	\$567,702,368	65.9%	\$27,394,362
Alexander Borodaev	\$291,012,050	69.2%	\$15,449,077
Sergey Uryadov	\$211,472,521	71.7%	\$10,776,607
Mikhail Irzak	\$180,762,590	66.1%	\$10,023,605
Boris Varshavskiy	\$44,241,487	63.9%	\$2,821,032
Rumiantcev	\$49,227,394	71.3%	\$2,192,460
M13	\$65,487,669	67.1%	\$2,402,509
Total	\$2,213,729,217	67.8%	\$121,923,901

Table 3: PJI Summary

	Gross MacDonald Profits	PJI	Total
Igor Sladkov	\$ 50,864,250	\$ 9,768,297	\$ 60,632,546
Mikhail Irzak	\$ 10,023,605	\$ 1,978,122	\$ 12,001,728
Rumiantcev	\$ 2,192,460	\$ 397,947	\$ 2,590,406
Total	\$ 63,080,315	\$ 12,144,365	\$ 75,224,680

	Quarter End Date	Gross MacDonald Profits	Quarter PJI	Total
Igor Sladkov	31-Mar-18	\$ 49,000	\$ 14,878	\$ 63,878
	30-Jun-18	\$ 177,205	\$ 50,959	\$ 228,164
	30-Sep-18	\$ 991,658	\$ 269,285	\$ 1,260,943
	31-Dec-18	\$ 1,059,249	\$ 270,871	\$ 1,330,120
	31-Mar-19	\$ 2,121,785	\$ 503,733	\$ 2,625,518
	30-Jun-19	\$ 2,921,557	\$ 640,347	\$ 3,561,904
	30-Sep-19	\$ 9,149,513	\$ 1,866,501	\$ 11,016,013
	31-Dec-19	\$ 18,381,691	\$ 3,474,507	\$ 21,856,198
	31-Mar-20	\$ 9,503,832	\$ 1,657,658	\$ 11,161,490
	30-Jun-20	\$ 3,992,224	\$ 638,756	\$ 4,630,980
	30-Sep-20	\$ 2,516,536	\$ 380,802	\$ 2,897,338
Total		\$ 50,864,250	\$ 9,768,297	\$ 60,632,546

	Quarter End Date	Gross MacDonald Profits	Quarter PJI	Total
Mikhail Irzak	30-Jun-18	\$ 112,051	\$ 32,222	\$ 144,273
	30-Sep-18	\$ 258,064	\$ 70,077	\$ 328,141
	31-Dec-18	\$ 232,555	\$ 59,469	\$ 292,024
	31-Mar-19	\$ 499,180	\$ 118,510	\$ 617,690
	30-Jun-19	\$ 1,068,046	\$ 234,094	\$ 1,302,140
	30-Sep-19	\$ 2,721,225	\$ 555,130	\$ 3,276,355
	31-Dec-19	\$ 2,352,346	\$ 444,640	\$ 2,796,986
	31-Mar-20	\$ 1,553,002	\$ 270,875	\$ 1,823,877
	30-Jun-20	\$ 854,126	\$ 136,660	\$ 990,786
	30-Sep-20	\$ 373,011	\$ 56,444	\$ 429,455
Total		\$ 10,023,605	\$ 1,978,122	\$ 12,001,728

	Quarter End Date	Gross MacDonald Profits	Quarter PJI	Total
Rumiantcev	30-Sep-18	\$ 79,156	\$ 21,495	\$ 100,651
	31-Dec-18	\$ 54,210	\$ 13,863	\$ 68,073
	30-Jun-19	\$ 204,769	\$ 44,881	\$ 249,650
	30-Sep-19	\$ 194,052	\$ 39,587	\$ 233,639
	31-Dec-19	\$ 282,733	\$ 53,442	\$ 336,176
	31-Mar-20	\$ 375,273	\$ 65,455	\$ 440,729
	30-Jun-20	\$ 871,061	\$ 139,370	\$ 1,010,430
	30-Sep-20	\$ 131,205	\$ 19,854	\$ 151,059
Total		\$ 2,192,460	\$ 397,947	\$ 2,590,406

Table 4: Probability to Trade on Potentially Hacked Events

	All IBES Earnings Events during Trading Period	Service- Provider Events	% of Earnings Events that are Service- Provider Events	Events Traded	Service- Provider Events Traded	Earnings Events Traded that are Service- Provider Events	Expected Number of Events Both Service- Provider Events and Traded, if Filing Agent and Trading Activities are Uncorrelated	p-value for Trades Uncorrelated with Release Filing Agent
Igor Sladkov	46,869	20,589	44%	386	375	97%	170	<0.0001
Mikhail Irzak	42,150	18,543	44%	495	484	98%	218	<0.0001
Vladislav Klyushin	38,359	16,810	44%	356	343	96%	156	<0.0001
Rumiantcev	38,063	16,660	44%	164	160	98%	72	<0.0001
Alexander Borodaev	32,004	14,085	44%	238	234	98%	105	<0.0001
Sergey Uryadov	25,307	11,147	44%	169	166	98%	74	<0.0001
Boris Varshavskiy	19,068	8,341	44%	149	147	99%	65	<0.0001
M13	18,799	8,330	44%	81	79	98%	36	<0.0001